A Wireless Network for Distributed Monitoring and Control

by

ALKESH KUMAR SINGH

DEPARTMENT OF ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY KANPUR

MAY 1997

A Wireless Network for Distributed Monitoring and Control

A Thesis Submitted

in Partial Fulfillment of the Requirements

for the Degree of

Master of Technology

by

Alkesh Kumar Singh

to the

DEPARTMENT OF ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY, KANPUR

May 1997

CERTIFICATE

It is certified that the work contained in the thesis entitled **A Wireless Network for Distributed Monitoring and Control** by **Alkesh Kumar Singh** has been carried out under ~~my~~ our supervision and that this work has not been submitted elsewhere for a degree

Dr K R Srinivathsan
Professor,
Department of Electrical Engineering
Indian Institute of Technology Kanpur

Dr M U Siddiqi,
Professor,
Department of Electrical Engineerin
Indian Institute of Technology, Kanp

May 1997

Acknowledgements

First of all, I would like to express my sincere gratitude to my thesis supervisors Dr K R Srivathsan and Dr M U Siddiqui for their invaluable guidance and constant encouragement throughout the work I would like to thank them for giving me complete freedom in work

I would like to thank Mr Reddy and Amit for their costant help and encouragement I would also like to thank all the members of Telematics group Ila Nigam Sandhyaji Bhatnagarji, Kaushal etc and especially Mr Navpreet Singh and Madam for their help during my thesis work

Words fail to express my gratitudes towards my Jijaji sisters (Chetna Didi & Reeta) and family members who so lovingly remain an unflinching source of encouragement in everything I do

I would like to thank all the friends of Telecom Networks and Communication Thanks to Mohit, Manoj, Kohli, Vipin and Srinivas for their good company in labs Thanks to Prakash Veer, Pawliwal, Sumeet and all others for their company in SBRA Thanks to Kapil Mohan Jaiswal, Bansal, Avi, Vishal, Jayesh Umesh Utpal Tomar Shukla and all other friends who made my stay in Hall 4 a memorable one Thanks to Suneeta Pratima and Nitu

Last, but not the least, I would like to thank all the IITK community for providing me with a peaceful ambience and a home away from home

Alkesh K Singh

Abstract

For monitoring and control applications, a reliable data communication network is a prerequisite. Since data acquisition often involves areas which are geographically dispersed or difficult to access, wireless networks are often preferred. The wireless networks, such as cellular system and VSAT, are widely being used for voice and data communication services. However, there are many applications where the cost of such network systems is high, or the capacity and response requirements are not adequate. Therefore, there is a necessity to develop an appropriate and economical network for monitoring and control of geographically distributed objects.

In the thesis, an attempt has been made to develop a low cost communication network for monitoring and control applications which exploits the capabilities of the existing radiopaging communication. The parameters needed to arrive at the design specifications of this network are assumed from both the available communication capacity and typical scenario of power distribution automation. Then, a network based on forward radiopaging and return walkie-talkie radio data link is propose . Since the radiopaging standard used (POCSAG) is for one way communication, it has been modified to suit the requirements of the network. The roll-call polling scheme with a suitable timing control technique is used in the network to gather the system information. Issues related to error-recovery are also considered. The proposed communication scheme has been implemented and tested over a communication interface for a PC specially developed for this purpose.

Contents

List of Figures

Chapter 1

Introduction

In many industry applications and monitoring of geographically distributed objects, distributed data acquisition and control is increasingly applied using new communication networks techniques. In industrial plants, the underlying network is usually a wired LAN suitable for harsh and real time environments. In the monitoring of geographically distributed objects, say using GIS, such as truck/taxi fleet monitoring, wireless networks such as cellular mobile telephony or low speed data networks via satellite (e.g. Qualcomm's OmniTRACS [Qual]) are being used. However, there are many applications where the cost of such network systems is high, or the capacity and response requirements are not adequate. Examples of such applications are power distribution system, petroleum industry, food and agriculture, water resources etc. In specific high volume application areas such as distribution automation, the development of an appropriate and ecconomical network for the monitoring of large number of geographically distributed objects and their control is worth considering.

In this thesis, a value added wireless network over existing paging or emerging reverse paging network paradigms suitable for the monitoring and control of geographically distributed objects is proposed. This network will be reffered to as *Wireless Network for Distributed Monitoring and Control* (WNDMC). The specific design considerations and implementation of the physical and MAC level schemes of this network are described. The proposed MAC scheme has been implemented and tested over a communication interface for a PC specially developed for the purpose. The parameters needed for arriving at the design specifications of this network are assumed from both available communication capacity and a typical scenario of power distribution automation.

1.1 System Architecture of the WNDMC

The proposed system architecture assumes a set of geographically distributed sites, each site with some equipments to be monitored and controlled from a *Master Station* as shown in Figure 1.1. A *Remote Terminal Unit* is placed at each site which acts as an interface between the master station and the system equipments. The master station and the RTUs are equipped with suitable radio transmitter and receiver for wireless communication. The master station may also be connected to other LAN/WAN.

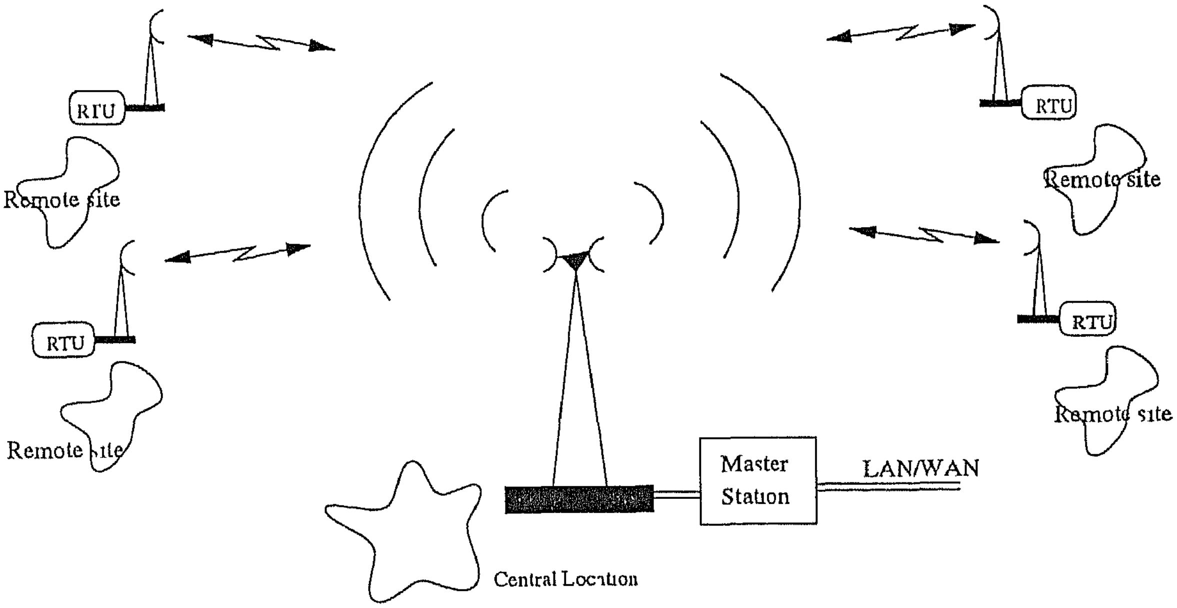


Figure 1.1: System Architecture

The telemetered information rate from each RTU is assumed to be on an average few bytes per second or less. The channel available is 12.5 KHz as approved by wireles authorties of India for such applications. Within the band, an approved signaling forma such as in paging is assumed.

In the case of power distribution system, the master station is assumed to be at manned 33/11KV substation and the RTUs are placed at unmanned 11KV/400V trans formers. The 33/11KV substation may futher be connected to a 66/33KV substation or to the power grid via appropriate communication network. The RTUs collect the information of current, voltage, power, temperature and other parameters form the transformer. The data transfer rate from unattended transformer (RTUs) is assumed to be small – of the order of a few bytes per second or less on an average from each unit to the master station. The distance of RTUs from master station may vary from a few hundred meters to 20 or 30 Kms. The data rate from the master station to RTUs is also assumed to be small – typically an occasional few bytes for polling and commands, answered by 100 bytes or so of report to the master station [KrRe]. Assuming a polling rate of once every 5 minutes per RTU and a maximum of 50 RTUs per 33/11KV substation, the communication rate can be easily accomodated in radiopaging bandwidth.

1.2 Wireless Technologies Suitable for WNDMC

Presently, there are many wireless communication techniques which can suit the requirements of diverse applications. However, in most of the cases there is a single technique which best suits the requirements of a system. In this section, we present a brief description of some existing wireless techniques which are being used for data or voice communication in many industries.

Cellular Communication

Cellular communication is one of the fastest growing technology which is being used for voice and data communication. The concept of cellular communication is the use of low power transmitters where frequencies can be reused within a geographical area. In this system, the area to be covered is divided into small 'cells', each cell uses a frequency band which is also used in other cells not adjacent to this cell.

The analog techniques used in the cellular system provide voice message transmission and allow voice message to travel through either 30 kHz (AMPS in 800MHz band) or 25 kHz (ETACS in 800MHz or 900MHz band) voice channels. To exploit the capabilities of AMPS cellular infrastructure, CDPD technique is developed. It is a connectionless service which uses idle time of voice communication and provides seamless data communication upto 19 2 Kbps [AMPS]

The standards for digital techniques such as GSM (800MHz band) or PDC (800MHz or 1 5GHz band) use CDMA or TDMA for channel access and voice or data transmission The digital technology offers some advantages over analog technology sush as ease of signalling, lower levels of interference, integration of transmission and switching, and increased ability to meet capacity demand [GSM, John]

The cellular communication system (analog or digital) is suitable if both data and voice communication are required In the cellular system, base station and transceiver units are complex and expensive too Since the cost of a monitoring and control system is directly proportional to the cost of an RTU, the cellular system becomes very expensive for most of the applications with low data rate requirement

Radio Trunking

Radio trunking is one of the oldest technique of communication which is widely being used by transport fleet operators, police, courier providers etc for data and voice communication It is a popular and successful methods of achieving the spectral efficiency Instead of having a single radio accessing a single channel, trunking allows that same radio to search for one clear channel out of many possible channels Trunking, therefore, refers to the automatic search for a clear (idle) channel among two or more possible channels Most of the trunked systems are in the 800 900 MHz band (APCO 16), some other systems use higher frequency bands [Trunk] for data transmission

The radio trunking is cheaper than the cellular communication and in the context of WNDMC, it has the potential of meeting the requirements of the system provided some value addition in the form of data transaction capability over select channels is developed over the existing infrastructure However it requires a number of channels for dynamic channel allocation For the applications where a single channel is sufficient to serve the needs of distributed objects and the length of data per session is also small, other options must be considered

Radiopaging

The radiopaging technology is cheaper than other mobile communication technologies. Like the cellular communication, the area to be covered by radiopaging service is divided into small cells or radiopaging zones. Initially it was developed for tone-only or short alphanumeric messages and was a one way service such as POCSAG standard [CCIR]. New standards also provide a two way communication. Besides providing message service, it is expected that it can be used for industry applications such as building and plant automation etc.

Since the focus is in those applications where the system requires a low data rate links between remote locations and a central location, the radiopaging (CCIR Radiopaging Code No. 1.) communication has been selected for the distributed data acquisition and control of remote objects. It has many features which make it suitable for low data rate wireless link applications. Some features of pager receiver and radiopaging are as follows:

- Powerful forward error correction capability embedded in paging technology.
- Data transmission rate of 512bps, 1024bps, 2400bps and 3200bps. Some pagers also support data rate of 6400bps.
- Suitable for UHF/VHF range and bandwidth requirement is only 12.5KHz or 25KHz.
- Depending upon the transmitter power, the coverage area may be several tens of kilometers.
- Commercially available and, lower cost and complexity than radio trunking or cellular communication.
- Approved by international groups such as RCSG and POCSAG, and by CCIR.
- A widely accepted standard.

Hence, a pager receiver unit is placed at each RTU to receive data from the master station. The pager units presently available in India do not support two way communication. Hence a means for reverse communication should also be provided at each RTU.

The best option to provide the reverse communication is to use the common WT radio link with data modems The walkie talkie transmitters are available at low cost and are suitable for the application Decoding of received data at the master station from the RTUs can be performed in hardware or software

1 3 Organization of the Thesis

The rest of the thesis is organized as follows In Chapter 2, we present a communication network and communication scheme for the WNDMC We discuss various communication related issues such as structure of master station and RTUs, modified roll call polling for channel access control, error handling procedure to ensure reliable data delivery etc In Chapter 3, we propose a communication protocol which provides two way communication between the master station and the RTUs The protocol is based on POCSAG standard and we have modified it to suit the network requirements We also discuss the code capacity of the designed protocol in the same chapter In Chapter 4, we present the details of hardware (serial synchronous interface card) and software implementation Chapter 5 concludes the thesis and gives direction for the future extension of our work

Chapter 2

Network Architecture of WNDMC

In this chapter, we propose a network for the system discussed in section 1 2 The network is based on forward radiopaging and return walkie talkie radio link Then we discuss a scheme for wireless communication between the master station and the RTUs of WNDMC We discuss various communication related issues such as *Channel (medium) Access Control*, error handling procedure, group calling procedure etc In section 2 1, we present a brief introduction of a monitoring and control system Design issues of the communication network are considered in section 2 2 Then in section 2 3, we present a communication network which meets the requirements of the WNDMC Finally in section 2 4, we discuss a scheme for communication

2 1 Introduction

A typical monitoring and control system provides system monitoring, system control and system management functions It provides real time monitoring of the utility system status Timely data increases system reliability and efficiency, and decreases the service time and loss due to abnormalities of the system Accuracy of the reported data and the meaning of real time differs from one system to another Generally, data sampling time varies from some milliseconds to some minutes and accuracy varies upto ten percent of actual data [Sca91]

The data related to operating parameters of the remote equipments is collected at a central location. The gathered data is processed and received information (or signals) is displayed for the use of a operator. The operator uses this information to make changes (telecommand) in the operating status of the system and if neccessary sends personnal to correct problems or adjust system operating parameters. A record of the information received from the RTUs is also maintained which is important for resource management related functions.

2.2 Network Design Issues

In the industry applications there are various sites/equipments at different locations to be monitored and control. The distance of the sites from the master station is assumed to be from a few hundred meters to some tens of Kms. Since the RTUs collect data from different types of equipments, length of data from different RTUs may be same or different. It may be required to get information of some RTUs (sites) more frequently than the others. The communication requirement is that the master station must be able to send/receive data over a wireless channel to/from the RTUs in a desired way.

The other important issues considered to design a MAC level scheme for the purpose are as follows:

- The wireless network should fall into one of the commercial standard and wireless authorities approved wireless services, well supported by the market in terms of availability, diverse supply sources and acceptable cost.

- Since the frequency allocation is a subject of debate, the technology should be capable of working anywhere from the frequency band of 100 MHz upwards to atleast one GHz, without substantial changes internal to transmitter and receiver or modulation methods.

- The scheme must provide an error free and reliable communication between the master station and the RTUs. If any RTU malfunctions, the master station must be able to identify the RTU and to detect/correct the problem.

- The wireless network should be able to provide an acceptable data rates for forward/reverse communication.

- Timesharing should be used for sending information from the master station to the RTUs as only one channel (broadcast) is available for forward communication. Similarly there is only one channel for reverse communication from the RTUs to the master station. Although, each RTU uses the same channel but it might not be able to listen the transmission from all other RTUs. The scheme must provide a way so that each RTU gets its turn to sent data to the master station.

- The master station must be able to address any RTU at any time to send the control information. This control information may be based upon the feedback obtained from the RTUs or may be an independent decision of the operator.

- The master station must be able to access data from any RTU at any time. This may be required after sending control information to the RTUs or when some abnormality is being controlled or may be operators decision or for monitoring purpose.

- If the same information is to be send to a group of RTUs then it would be a wastage of bandwidth/time to repeat the same information for each RTU. A group/global address should be provided for common information transmission.

2.3 Network Architecture

The proposed network consists of a master station and many RTUs at remote locations as shown in Figure 1.1. Since the network is wireless, the master station broadcasts the information for the RTUs. All the RTUs listen to the transmission, but only those which are addressed receive the information. On the other side, transmission from the RTUs is received only by the master station. The communication related requirements of the master station and RTUs are as follows.

Remote Terminal Unit

The main components of an RTU are a communication controller, a processor, an interface to switches, meters, transducers, other analog and digital devices and, transmitter and receiver units. It acts as an interface between the master station and the system equipments. It collects data from the system equipments and carries out some processing to put the data in a format suitable for transmission. The data is transmitted when the RTU is polled by the master station. The RTU also receives commands from the master station to control the system parameters. The RTUs can also take independent decisions in emergency.

To suit the requirement of the control and monitoring network, the radiopaging network may use 12.5KHz bandwidth for forward communication (master station to RTUs) in the VHF or UHF spectrum. The return network of all embedded WT radios (transmitter only) can share one 12.5KHz bandwidth in the same band far enough to meet isolation requirements. Based on the model of a forward paging network and return radio data link, the block diagram of a typical RTU with wireless communication takes shape as shown in Figure 2.1.

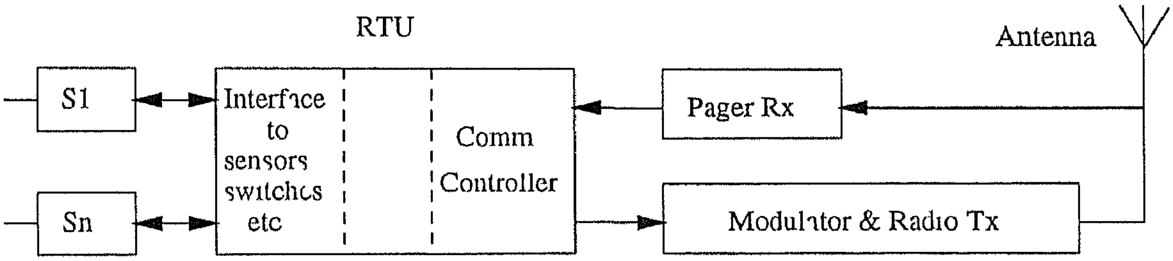


Figure 2.1 Architecture of RTU

Master Station

The master station consists of a communication controller, control panel and transmitter and receiver units. It gathers data from the RTUs using an appropriate polling schedule as discussed in section 2.4.2, carries out processing to extracts information of the system parameters and displays the information on a GUI (or uses LEDs, alarm etc.) for use of the operator. On detecting abnormalities, it may send control information to the RTUs if it is programmed. It also implements the operator's decision and maintains a record of data the from each RTU.

The master station has a paging base satation for the forward link to send commands to the RTUs and a radio receiver for the return radio data channel. The transmitter/receiver channels are controlled by a single communication controller. On one side, the communication controller communicates with radio receiver and pager transmitter and on the other side, it communicates with the master station over a LAN or serial link. The architecture of the master station is shown in Figure 2.2.

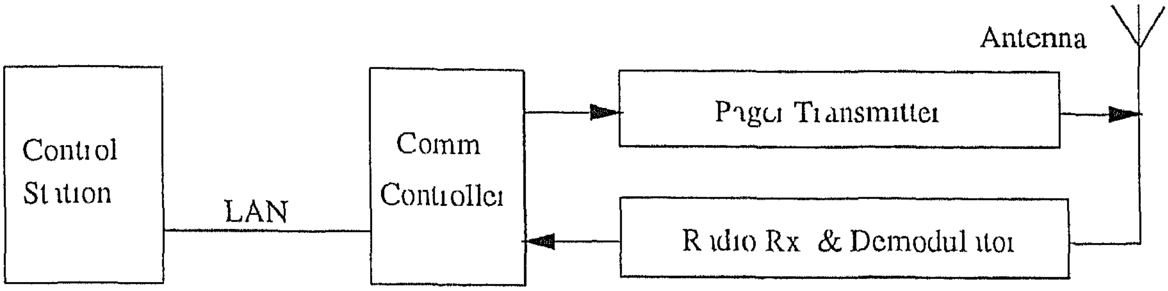


Figure 2.2: Architecture of Master Station

2.4 Strategy for Communication

2.4.1 Radio Paging Standard

Radiopaging is the most suitable technology for WNDMC as discussed in section 1.2. Several standards such as POCSAG, ERMES and FLEX are being used world wide for radiopaging. The proposed scheme is based on CCIR Radiopaging code No 1, also known as POCSAG standard, which is given in Appendix A [CCIR]. The transmission pattern and codeword structrue used in the POCSAG communication is shown Figure 2.3. To increase effective data transmission rate, without making substantial changes in the receiver hardware, we propose the following modifications in the transmission pattern,

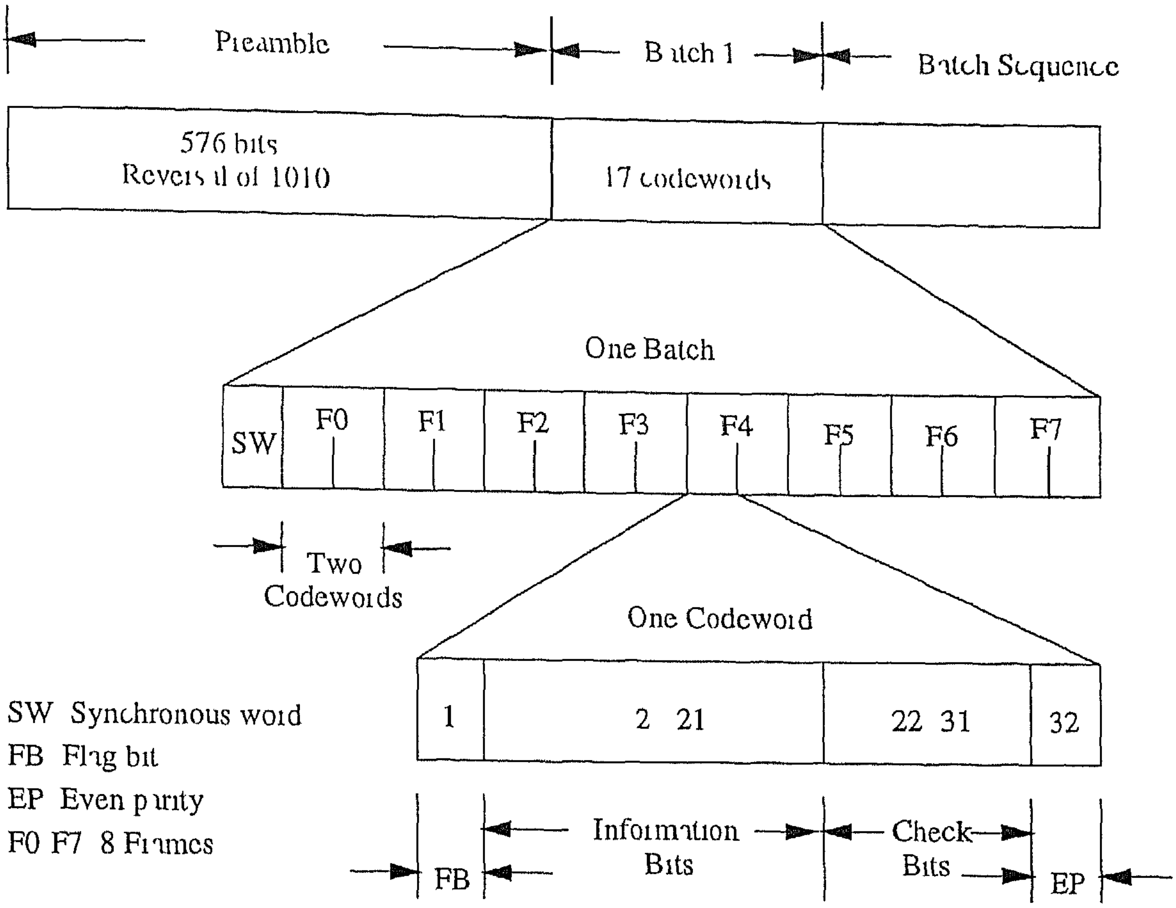


Figure 2.3 POCSAG Codeword Structure

- Length of the preamble can be reduced from 576 bits to 64 bits. In the pager, the receiver power is turned off for about 1 second whenever it detects no transmission. In this time it can miss 512 bits at a rate of 512bps. Moreover when it turns on, it can miss some initial bits. Hence, 64 bit preamble is enough for the application as receiver doesn't turn off when no transmission is detected.

- The framing in the batches can be avoided because it is used to increase the number of addresses available and for battery saving.

- Address of any RTU can be transmitted in any codeword place because pager power is not turned off during 'no transmission' time or during reception.

- In radiopaging application, receiver ceases decoding when two consecutive code words are indecipherable but in this application decoder will cease decoding if any codeword is indecipherable. Hence, it is not neccessary to put an idle or address codeword between end of one command' and address of second receiver.

2.4.2 Channel Access Control

There is one broadcast (wireless) channel for forward communication and only one transmitter at the master station, hence the channel can be used by the master station in any desired way to send commands to the RTUs. On the other side, there are many RTUs sharing a common channel for reverse communication. A way for accessing channel must be provided so that each RTU gets its turn to send information to the master station.

Several multiple access and line control technique are being used in various networks [Gal]. Due to the network requirement and receiver hardware, the mutiple access techniques FDMA and TDMA are not suitable. Among the line control techniques popular ones are,

1. Contention
2. Token passing
3. Polling

Token passing does not suit to the network as the RTUs do not listen to each other. Contention, on the other side, may prevent successful data acquisition in some critical condition as it is the master station which detects the collision and not the RTUs. The roll call polling has many features which make it suitable for the network. It (Figure 2.4) is essentially based upon the master slave relationship of network nodes, one master and all other nodes its slaves. The master sequentially polls the slaves to determine if they are ready to transmit/receive information to/from the master. The master has a poll list that can be manipulated to control polling priority and timing. Rules of this scheme govern the dialogue, also known as Handshaking, between the master and the slaves, which proceeds similar to the following. If the master wants to send data to a station C, it sends a poll to C asking if C is ready to recieve. C responds with an ACK if ready, allowing the master to send data, otherwise with a NACK. A similar dialogue takes place when master needs information from a station [Meye, Schw].

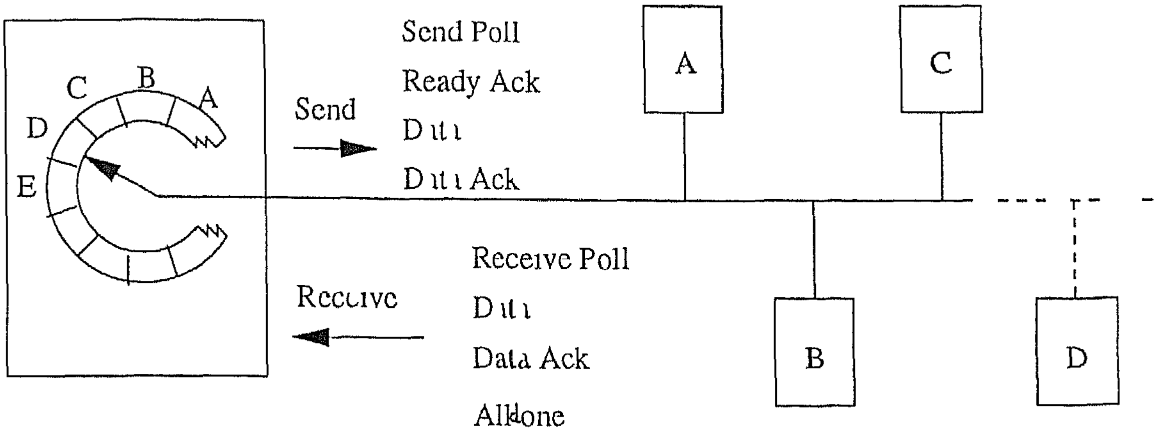


Figure 2.4 Roll call Polling

In the network, the master station is assumed to be a master and all the RTUs its slave. Polling scheme is same as described above with a difference that there is no handshaking. The control station has complete controls over the transmisssion channels. It sends commands to the RTUs and polls them. Whenever an RTU is polled, it has to send the information required by the master station. Thus, the same reverse channel is used by all the RTUs on time sharing basis controlled by the master station.

The master station polls the RTUs at a ragular interval to access the operating parameters of the equipments connected to the RTU. Depending upon the task performed by the equipments connected to the RTUs, the master station needs data from some the RTUs more frequently than the others. Hence, the polling interval is different for different RTUs. In polling, this is provided by providing lesser polling interval to some RTUs over the other. The RTUs which have equal polling interval and are connected to the same type of equipments are grouped together and the master station polls them after a regular interval.

2.4.3 Timing Control

The polling scheme is generally used in those networks where there is only one channel for reverse and forward communication. The master polls one slave and waits for the response, after receiving data from the slave it polls others. Obviously, if there are two seperate channels for each direction then this scheme is inefficient utilization of both channels

For better channel utilization instead of one slave a group of slaves is polled While these slaves send data to the master, the master sends commands on the other channel Thus the master continues to send data on the forward channel while it is receiving data on the reverse channel from the RTUs This modified roll call polling requires two extra features to be provided One, the master station must know the length of data transmitted by a RTU and second, the RTUs must receive proper *timing information* from the master station to send data at an appropriate time

Each RTU has a fixed number of devices and the state of each device is represented by a fixed number of bits/bytes The master station is provided with the information of the number and types of the devices connected to each RTU It may be required to add or remove some devices from the RTU but whenever any change is made, this is informed to the master station All this enables the master station to find out the total number of bytes needed by that RTU to send the local information

The master station may also inform the RTUs to send urgent information, detailed information etc as discussed in section 3 3 1 In each case, the RTU knows which information is to be transmitted and how many bytes it should transmit However, in some cases, it may not be possible to provide the master station with the information of data length from the RTUs In such cases, the master station assumes that the RTU will transmit the maximum number of bytes say 115 bytes Hence, when the master station polls one or more RTUs it knows when a particular RTU starts and (possibly) stops the transmission

The RTUs are located at different distance from the master station Depending upon the distance from the master station, the RTUs receive data at different time and accordingly they start transmission As shown in Figure 2 5, data from the two RTUs may overlap if one RTU stops transmission at a time T_2 and another starts transmission at the same time The overlapping period will be double if forward transmission time is also considered The following scheme can be used to avoid the data overlapping

During the initialization phase, the master station finds the round trip delay for each RTU Suppose, the maximum round trip delay is t If t_i is the round trip delay for an

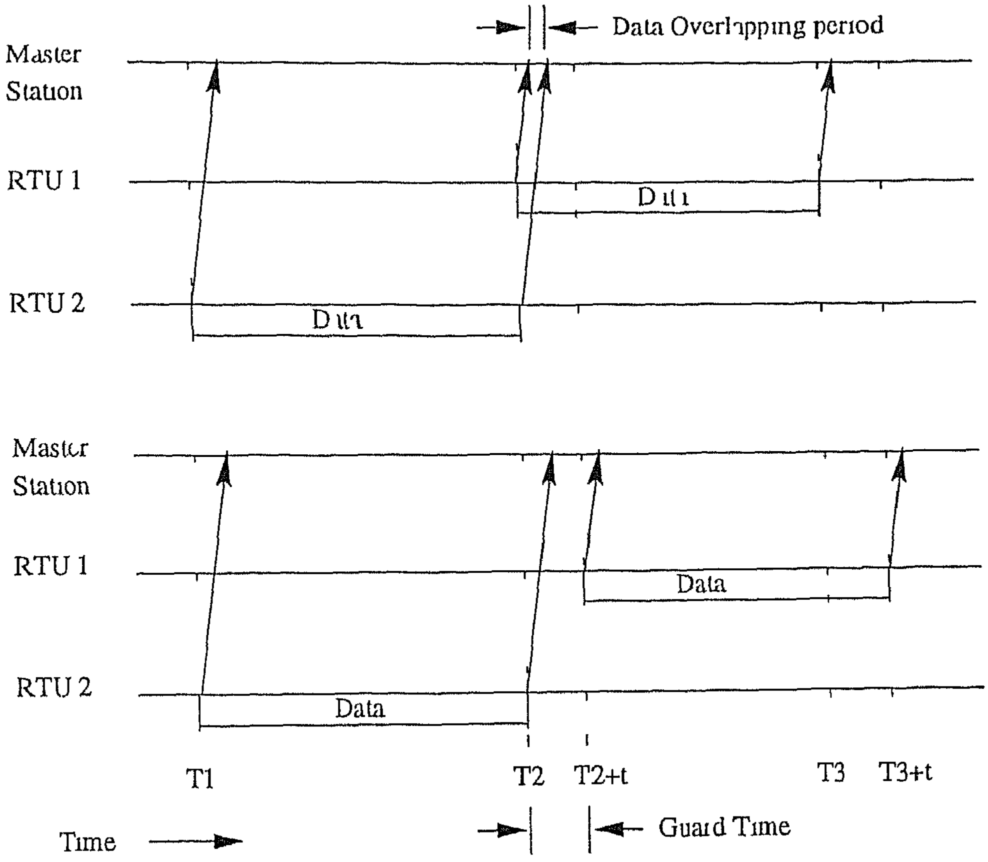


Figure 2 5 Data Overlapping

RTU, the master station sends a number equilent to $(t - t\prime)$ time to that RTU Now, whenever this RTU has to send data at time T, it start transmission at time $(T + t - t\prime)$ Thus the master station receives a continuous data stream from the polled RTUs in proper time synchronization as if it is comming from a single RTU This scheme requires complex hardware and advanced synchronization techniques at the master station and RTUs It makes the implementation part more difficult and also doesn't lead to a cost effective solution At the same time, transmission format (batch structure) can not be maintained as more than one RTUs are involved in the transmission A better approach would be to poll the RTUs in increasing order of their round trip delay However, it doesn't eliminate the need of estimating the round trip delay and at the same time, data on the reverse channel in not synchronous The following scheme is a better solution for timing control

A guard time is provided between transmissions from any two RTUs (Figure 2 5) If one RTU ends transmission at time T_2 then the master station informs to the next RTU to start transmission at time T_2 + t, where t is the guard time. Whenever the master station polls an RTU, it finds the number of codewords to be transmitted by other RTUs which are polled before this RTU and the guard time for all those RTUs. If n RTUs are polled before a particular RTU then the number n along with N, representing total number of codewords to be transmitted by other RTUs, is send to that RTU. In this way, the RTU receives the *timing information* and starts transmission after T_w time where

$$T_w = (n * guard\ time + N * word\ transmission\ time)$$

2.4.4 Error Handling Procedure

The pager receiver at the RTU is able to correct double errors in a packet of 32 bits. Due to random nature of channel noise and ambient conditions, more than two errors may occur in a packet and the receiver may not be able to correct errors. Hence, to ensure reliable data delivery, the master station requires an acknowledgement from the RTUs for each control command transmitted. Sometimes, however, the master station may not decode data from the RTU or an RTU may not detect its address, hence it will not respond to the control command. In such cases, the master station may retransmit the control command. However, this is an unneeded transmission if the RTU has already received the command. An acknowledgement command, which does not carry the control command but informs the RTU to send acknowledgement for the previously received control command, does not solve this problem.

To overcome the problem, a numbering scheme can be used such that whenever a command is transmitted to an RTU it also carries command number which is incremented by 1 (mod N) for each new command to that RTU. The transmission of the command number with each command can be avoided if the RTUs and the master station agree on some initial command count. If both agree on initial count zero than both increase the count by one for each command transmitted/received. Whenever the master station needs an acknowledgement, it sends the *control command number* (CCN) for which acknowledgement is required.

As described in Chapter 3 CCN is sent with each control command. With this command a *timeword* is also transmitted which carries the *CCN, timing information* as well as some other information.

An other problem arises if any RTU is unable to transmit/recieve data to/from the master station. In this case, the master station does not get any acknowledgement or any response from the RTU. Actually, if the master station doesn't get any response from the RTU, it retransmits the information and continues to retransmit until it gets a response or a maximum count of retransmissions is reached. If it gets a response, it continues with other tasks and if the maximum count is reached, it sends a signal to the operator who takes appropriate action.

2.4.5 Group Calling

Although the POCSAG standard provides four different addresses to each pager receiver but it doesn't provide a common address for a group. The addresses of one receiver are always diffirent from the addresses of other receivers. Hence, two or more receivers never receive same data. To send a common information to a group of RTUs their addresses ~~sequentially~~ are transmitted sequencially. Then the information is transmitted so that each receiver of the group receives it. In this case, each receiver should know that information for a group is being transmitted otherwise it will stop decoding upon detecting a second address. Hence, to send information to a group, address of one RTU followed by a timeword is transmitted for each RTU. The address informs the RTU that a command for a group is being transmitted and the timeword carries the information of the time of 1*st* command codeword as well as *command number*.

2.5 Discussion

In this chapter, we discussed the issues related to the network design and communicaion scheme. Since in the network, the RTUs are placed at fixed locations, the power transmission requirement of the RTUs can be reduced by using directional antennas. It may also reduce the preamble length needed from the RTUs. However, actual minimum preamble length can be determined only by field experiments

In the chapter we discussed only those requirement which are necessary for two way reliable communication The efficiency and reliabilily for the network can further be improved at the cost of increased cost and complexity For reliable communication, one of the basic technique was used It seems that sending command number with each command will consume some bandwidth but as we will see in next chapter, it is sent with the *timing information* in a single codeword The *timing information* is sent in such a way that only single clock generator is sufficient to fulfill the needs of transmitter and the down counter which is loaded with an appropriate number equilent to T_w time This method also avoids the need of a real time clock and provides better time synchronization as the time is relative

It is obvious from the description that the requirements cost, complexity etc of the proposed network and communication scheme for WNDMC are far less that the requirements of a cellular or other networks for the same

Chapter 3

Communication Protocol Design

In this chapter we propose a communication protocol based on the techniques discussed in the chapter 2 for communication between the master station and the RTUs Since the traditional radiopaging is for one way communication, we propose some modifications in the POCSAG format to suit the requirements of WNDMC Without altering the general transmission pattern and codeword structure used in POCSAG, we redefine the codewords and their significance We describe the data transmission patterns from the master station and the RTUs Some common errors that are expected to occur in communication and procedures to overcome these errors are also described Then we calculate approximate capacity of the described protocol under some assumptions

3 1 Introduction

Before transmitting data from the master station or RTUs, some operation are performed on the data to put it into a defined format As shown in Figure 3 1, information from the data source passes through different blocks before final transmission The information to be transmitted from the data source is passed to the codeword generator The codeword generator devides the data into blocks of 20 bits and pads 0's if necessary In each block, it adds some bits, a flag bit to indicate that this is a *data codeword'* and 11 check bits for error control, and make a 32 bit codeword The frame generator (a batch in the POCSAG will be refered to as a *frame*) takes the codewords and puts them into a batch or frame of 17 codewords as defined later in the chapter. It also puts an address(s) codeword and synchronous words at appropriate places in the frames. The *address code words'* are also generated in the same way as the data codewords except that the flag bit indicates that it is an address codeword. The transmitter starts transmission with a preamble and then transmits the frames received from the frame generator. In the next section, we describe the structures of the codewords, frames and transmission pattern etc.

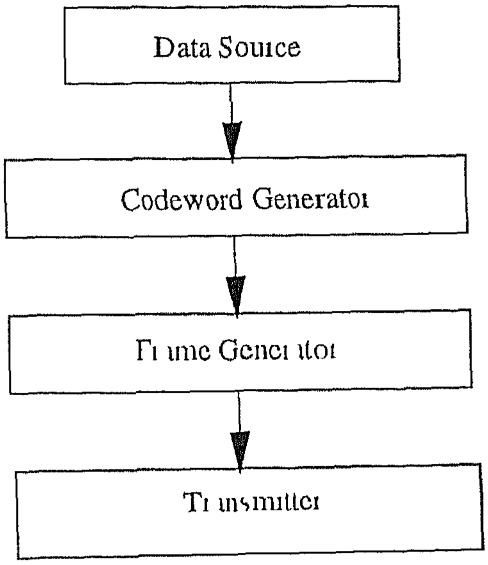


Figure 3.1 Data Sequence Generator

3.2 Code and Format

3.2.1 Codeword Generation

The coding technique used for codeword generation is BCH and the code used is (31 21) BCH code with added even parity bit. Thus, each codeword contains 32 bits, 21 information bits and 11 check bits. The informations bit either contain a 20 bit address or 20 bits of data.

The generator polynomial for this double error correcting code is,

$$g(x) = x^{10} + x^{9} + x^{8} + x^{6} + x^{5} + x^{3} + 1$$

Suppose m(x) represents the 21 information bits, then it is a polynomial of degree 20. The following division gives 10 check bits for the codeword,

$$c(x) = m(x)\,x^{10}/g(x) \qquad \text{(modulo2 division)} \qquad (3.1)$$

and

$$t(x) = m(x)\,x^{10} + c(x) \qquad (3.2)$$

where t(x) is 31 bit codeword. One extra bit is added to this block of 31 bits to give overall even parity. Thus the code becomes (31,21 BCH + 1 even parity) a block of 32 bits.

The Hamming distance of this code is 6. Hence it can correct any 2 random bit errors and can detect any 5 random bit errors. A detailed description of decoding and encoding procedures of the BCH codes codes is given in [Blah].

3.2.2 Types of Codeword

Each codeword contains 32 bits and is transmitted with the most significant bit first. Different types of codewords are as follows:

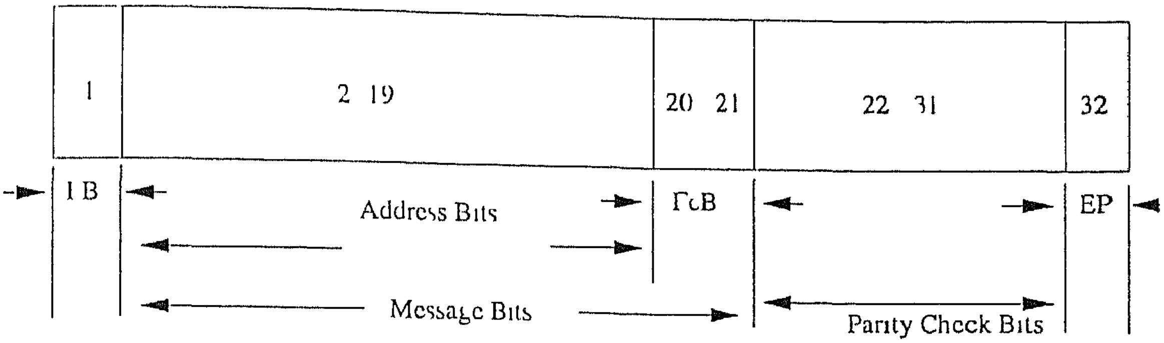
a. Address codeword

General structure of a 32 bit *address codeword* and *data codeword* is shown in Figure 3.2.

Bit 1 is flag bit used to indicate address/data codeword. This bit is 1 for data codeword and 0 for address codeword. Next 18 bits (2-19)are address bits used to identify a particular receiver. Next 2 bits (20-21) are function bits. These bits provid four addresses to each receiver. Bits 22-31 are check bits. They provide overall 2 bit error correction capability to each codeword. Last bit is overall even parity bit.

The 2 function bits provide four addresses to each receiver. All four addresses can be used either by the master station or by the RTUs. These addresses are difined as follows:

- **Individual address (Ind_Add)**: The function bits for Ind_Add address are 00. This addresses is used by the master station to send control commands to a single RTU and by the RTU to request for retransmission.



FB Flag Bit
FcB Function Bits
EP Even Parity

Figure 3 2 Codeword Structure

- Group address (Grp_Add) The function bits for Grp_Add address are 01 This is used by the master station to send control commands to a group of RTUs and by the RTU to request for group command retransmission

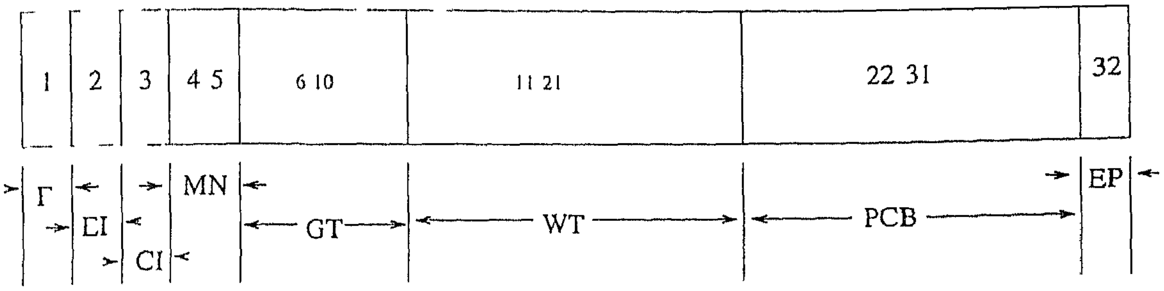
- Acknowledgement address (Ack Add) The function bits are 10 for Ack_Add Whenever master station wants an acknowledgement for the previous transmission, it sends this address An Ack_Add from the RTU implies sucessful reception of thE command

- Poll address (Pol_Add) The function bits are 11 for Pol_Add This codeword is used by master station to poll the RTUs and by the RTUs to send system information

b Data codeword

The structure of a *data codeword* is similar to that of an *address codeword* as shown in Figure 3 2 In this case, 20 bits (2 21) are information bits and the flag bit is always 1 The length of commands may be more than a frame but the general frame structure is not altered The commands may embrace more than one frame maintaining the synchronous word at first codeword place c Other codewords

A timeword is a *data codeword* It is used to carry the timing information, message number etc for the RTUs The general structure of this codeword is shown in Figure 3 3



F Flag bit

EI End Identifier

CI Counter Identifier

MN Message Number

GT Guard Time

WT Word Time

PCB Parity Check Bits

EP Even Parity

Figure 3 3 Timeword Structure

Bit 1 of the timeword is always 1 indicating that it is a data codeword Bit 2 (=1) indicates command termination and is 0 otherwise Bits 3 6 are used either to indicate the type of polling as defined later or as follows Bit 3 is counter indentifier bit and bits 4 5 carry command number of the current command Bits 6 10 are for the calcucation of guard time delay and bits 11 21 are for the calculation of codeword transmission time An idleword is transmitted when there is no command to transmit or to indicate end of command Bit contents of idleword are given below

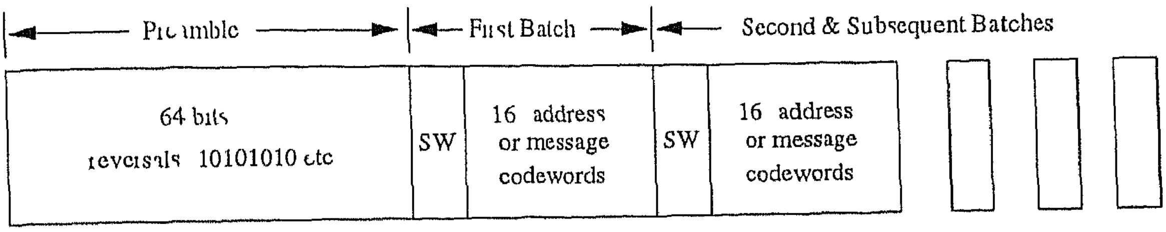
01111010100010011100000110010111

A synchronization word is same as defined in POCSAG Its first 31 bits are a PRBS which can be generated from a five stage feed back shift register It is a valid address outside the required range The bit sequence for the word is,

01111100110100100001010111011000

3 2 3 Frame Structure

The codewords are structured into frames which comprise a synchronisation codeword followed by 16 codewords The frames are transmitted after the preamble First code word of the frames is always a synchronisation word and the rest 16 are *address codewords* or *data codewords* Address of any receiver can be transmitted in any frame and in any codeword



SW Synchronous Word

Figure 3 4 General Transmission Pattern

A general transmission pattern shown in Figure 3 4 The transmission always starts with a preamble to synchronize the receiver which is followed by a frame sequence The minimum length of preamble in POCSAG standard is defined to be 512 bits at a rate of 512 bps For the reasons already defined in section 2 4 1, the length of preamble for the application has been reduced to 64 bits

3 3 Forward Communication

As discussed in section 2 4 2, the master station has complete control over the forward and reverse transmission channels It establishes sessions with the RTUs to poll them or to send control information It also implements the decisions of the operator Different communication related functions performed by master station can be classified as follows,

- Actions initiated by the operator
- Real time polling and control

- Error handling

In this section, we focus on the first two function The error handling procedure is discussed after describing the reverse communication

3 3 1 Actions initiated by the operator

The operator polls the RTUs, sends control commands to a single RTU or to a group of RTUs and informs the RTUs to send an acknowledgement for the previously transmitted commands The master station receives the commands from the operator and establishes sessions with the RTUs For each session a particular set of events occurs The master station starts transmission with the preamble (if it is in idle state) which is followed by the frame sequence Each frame consists of a synchronization word (SW) and data/address codewords The *frame structure* and the possition of SW in the frames is always maintained The transmission patterns for different sessions are as follows (response from the RTUs is described in next section)

1 Command Words to RTUs

The operator sends commonds to the RTUs to control the system parameters He also needs acknowledgement from the RTU for the commands transmitted In this case, an Ind_Add and a timeword followed by the data codewords are transmitted The bit contents of the timeword are as follows, *2nd* bit is 0, *3rd* bit is 1, bits 4-5 carry the *command number* and bits 6 21 carry *timing information* The *command termination* is indicated by the idleword After the idleword, address of any RTU may be transmitted A typical transmission pattern is shown in Figure 3 5,

Preamble	S W	Ind_Add	Time word	Command words	Idle word	Ind_Add	Time word	Command words	Idle word

Figure 3 5 Transmission Pattern 1

2 Command words to a group of RTUs

One address can not be assigned to more than one RTUs As discussed in section 2 4 5, the RTUs of a group are individually addressed by the Grp_Add which is followed by the timeword The timeword carries the data transmission time and the CCN of group command (3rd bit of timeword is 0) In this way, each RTU of the group first receives the time of *1st data codeword* and then receives the data Message termination is indicated by the idleword A typical sequence is shown in Figure 3 6,

Grp_add add # 1	*Timeword*	Grp_add add # 2	*Timeword*	*Message words*	*Idleword*

Figure 3 6 Transmission Pattern 2

3 Polling Session

The operator can poll any RTU at any time for the information of the all/selected devices connected to the RTU

The transmission consists of a Pol_Add and a timeword The *2nd* bit of the timeword is 1, indicating the command termination Bits 3 5 can have 8 different bit patterns According to the need of a particular application these ~~nine~~ bit patterns may have different significance, say the bit pattern for normal information is 000, for urgent information is 001, detailed information is 010 etc It is not neccessary to use all the bit patterns and some might be reserve for future use Bits 6 21 carry the *timing information* A typical transmission pattern is shown in Figure 3 7,

POL_ADD # 1	*Timeword*	POL_ADD # 2	*Timeword*	POL_ADD # 3	*Timeword*	POL_ADD # 4	*Timeword*

Figure 3 7 Transmission Pattern 3

4 Acknowledgement Session

Acknowledgement may be required for the commands transmitted to a single RTU or to a group of RTUs For each case, Ack_Add followed by the timeword is transmitted The timeword carries the information of type of acknowledgement needed and the CCN in the following way bit 2 of the timeword is 1, bit 3 is 0 if acknowledgement for group command is needed and 1 for individual command, bit 4 5 carry the CCN and bits 6 21 carry *timing information* A typical transmission pattern is shown in Figure 3 8,

Ack_Add add 1	Timeword	Ack_Add add 2	Timeword	Ack_Add add 3	Timeword

Figure 3 8 Transmission Pattern 4

3 3 2 Real time polling and control

For real time polling, the RTU are devided into smaller groups and each group is polled periodically This period may be different for different groups and is assumed to be of the order of a few minutes for each group The master station polls one group on forward channel, receives data on reverse channel and sends the data to a control programmme It also maintains a record of data received from each RTU While it is receiving data from one group on reverse channel, it continues to send commands over the other channel Since the master station has some estimate of data from each RTU, it polls the RTUs in such a way that both of the channels are optimally utilized

In some applications, it may be required to collect some detailed or urgent information from each RTU after a certain interval This information is proveded to the RTUs by bits 3 5 of the *timeword* The master station itself can send commands to the RTUs on detecting some minor abnormalities in the system if it is programmed The commands are transmitted in the same way as discussed in section 3 3 1 Otherwise, on detecting any abnormality in the system parameters it call the operator by an appropriate alarm or display

3 4 Reverse Communication

Each RTU always listens to the master station On detecting its address it starts decoding the codewords directly following the address codeword It continues to decode until it receives a codeword indicating the command termination, an address codeword or an invalid word

If the RTU receives its *address codeword, data codewords* and a *command termination word* (timeword or idleword) successfully, it indicates a normal termination of command {If the commands themselves can indicate the *end of command*, as the timeword does, the *command termination word* (idleword) has no significance In this case, on detecting end of command the RTU will record it as a normally terminated command whether it receives idleword or not }

If the RTU decodes *address codeword* successfully but before receiving a *command termination word*, it receives an *address codeword* or it is unable to decode a word, it indicates an abnormal termination of command

The RTU sends acknowledgements for the commands received Therefore, for each command it records the *command number* and whether it was received correctly A 6 bit register is enough to keep this record Three bits are used to keep record of individual commands and three bits for group commands First bit of each register (depending upon the type of command received) indicates whether the last command was received successfully and the rest of the two bits contains the *command number* The RTU updates one register for each command received from the master station The RTU looks at these registers whenever it has to send acknowledgement to the master station The RTU also has to send system information to the master station in response to poll It responds in the following way

1 Response to Pol_Add

In response to poll command, the RTU has to send information of devices connected to it It calculate the time of transmission from the information contained in the received *timeword* and also looks at the bits 3,4 and 5 of the word to check which data is to be send It always starts transmission with the preamble and *synchronization word* to synchronize the receiver at the master station The SW is followed by the Pol_Add and data It also sends an idleword as an end of command identifier

2 Response to Ack_Add

For Ind_Add commands and Grp_Add commands, the RTU records the command number and status of reception If it receives a command successfully, it sets the corresponding bit to 1 otherwise it resets the bit

While responding to Ack_Add the RTU transmits the preamble and two codewords The first codeword is a *synchronization codeword* and the second depends on the type of received command If an acknowledgement is needed for the group command, the RTU checks the *command number* in the received *timeword* and the recorded *command number* If both the numbers are same and the status bit is 1, an Ack_Add is sent Otherwise, it sends the Grp_Add The same procedure is followed if acknowledgement is needed for the command sent to a single RTU The only difference is that an Ind_Add is sent instead of a Grp_Add

3 Response to Ind_Add Commands

Each RTU has to send acknowledgements for the commands received with Ind_Add The response is similar to Ack Add commands If the RTU receives Ind_Add, timeword and commad words sucessfully, it sends an Ack Add If it receives only the Ind_Add and the timeword, it sends Ind_Add In other cases, it does not responds

3 5 Error Handling

The POCSAG code format used for communication itself provides double error correction capability to each codeword In case of more than two errors in a single codeword the receiver can not decode the codewords Hence we consider only those cases when more than two errors occur in a codeword

In the forward direction, two types of error may occur first an RTU doesn't recognize its address, second the RTU is unable to decode a data codeword In first case the RTU doesn't know whether any command was transmitted for it Hence it does nothing In second case, although it knows that the command could not be received but being a slave in the network it has no way to start an error recovery procedure It only updates the status register if it receives the Grp Add or the Ind_Add before receiving an invalid word

On the other side the master station is responsible for all error recoveries Therefore, it maintains some status registers to keep record of session with each RTU It needs response from RTUs for all the commands For each command it updates one of the registers Bits needed for each register and their significance are as follow The Grp_Add and Ind Add registers are 2 bit registers One of the registers is incremented by 1 (mod 4) for each control command sent to the RTU

The Pol_Add register and the Ack_Add register are 1 bit register The bit in the register is set to 1 when the master station polls an RTU or sends an acknowledgement command to an RTU The master station also stores the last transmitted individual and group commands for each RTU The command is retransmitted if it receives a NACK from the RTU

One more register is used to count the number of retransmissions of poll and Ack_Add commands This register is incremented by one for each retransmitted command (poll or Ack_Add command) The master station continues to retransmit until it receives a positive response from the RTU or a maximum count of retransmissions is reached This maximum count might be different for different RTUs because RTUs are located at different place in the network and depending upon the distance call success rate is different This count should be lesser for the RTUs which are nearer and should be determined experimentally Anyway, if the maximum count is reached the operator is called for appropriate action otherwise the register is set to 0

3 6 Code Capacity Approximation

In this section we calculate the approximate capacity of the code described in this chapter The following analysis assumes that the transmission baud rate from the RTUs is 512 bps and no error occurs in the transmission channel All the RTUs of the network are similar i e they have equal data to transmit on each poll and polling interval is also equal for the all RTUs The guard time is assumed to be equal to one bit duration It is also assumed that the RTUs are polled in such a way that the reverse channel is optimally utilized

Suppose total number of RTUs in the network = n,

Polling interval for the RTUs = t seconds,

Data to be transmitted from each RTU = x bits,

A simple calculation shows that N (data bits + redundant bits), total number of bits to be transmitted from an RTU can be written as

$$N = 128 + \left\lceil \frac{x+40}{320} \right\rceil * 32 + \left\lceil \frac{x}{20} \right\rceil * 32 \qquad (3\ 3)$$

Hence, total number of bits transmitted from all the RTUs per polling interval are nN Since the guard is equal to one bit duration, the time taken by all the RTUs to transmit their data is equal to (nN + n) bit duration Hence, the minimum polling interval t is,

$$t = \frac{n(N+1)}{512} \qquad (3\ 4)$$

For the fixed number of RTUs, above equation shows a trade of between the polling interval and number of data bits which can be transmitted from each RTU The equations also show that there are small regions in which the polling interval remains constant irrespective to the number of bits transmitted from each RTUs A graph showing the relationship between the polling interval and number of data bytes which can be transmitted from each RTU per polling interval is shown in Figure 3 9

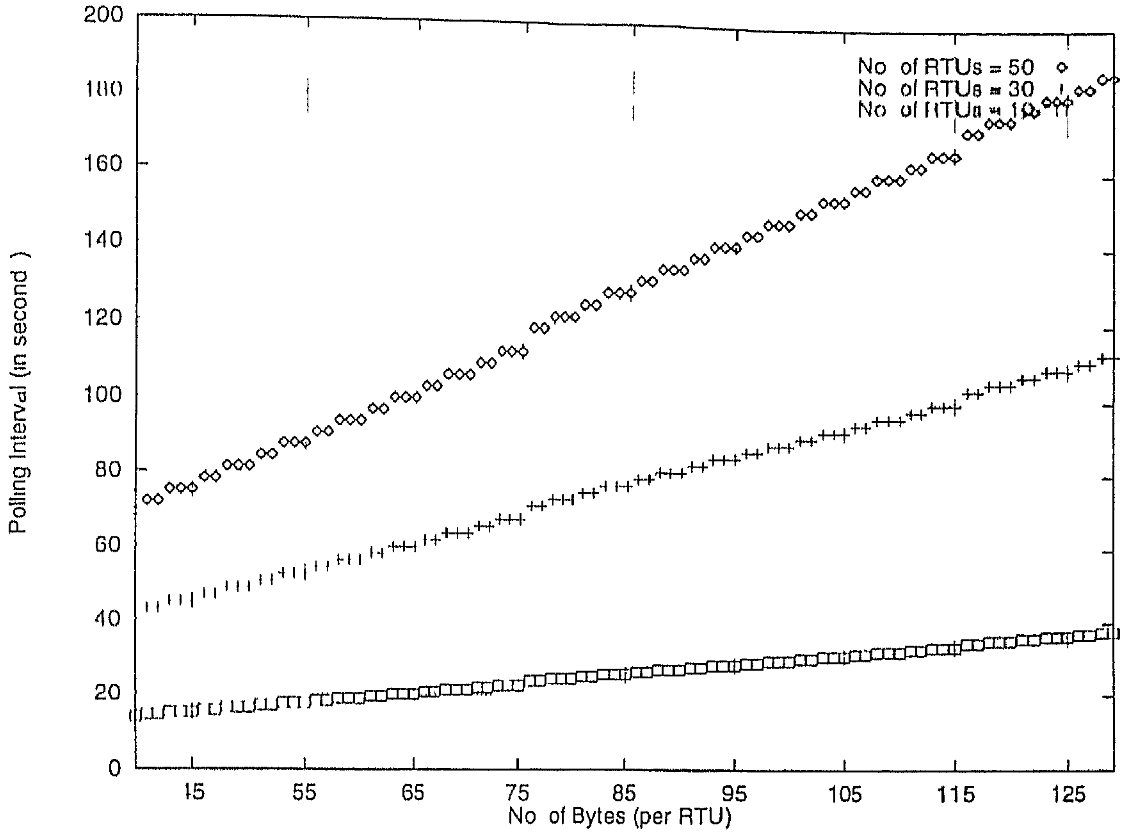


Figure 3 9 Code Capacity

Since the channel is not error free as assumed above, we calculate the probabily that the data of length N bytes from an RTU will be received at the master station without any error The codeword structure provides the data decoder with the capability to correct upto two errors in a codeword For a bit error rate of p, the probability of two of fewer errors in a 32 bit codeword is, for independent errors,

$$P = \sum_{i=0}^{2} C_i^{32} p^i (1-p)^{(32-i)}$$

Hence, probability that c codewords will be received with two or less errors is P^c A graph showing the relationship between the probability of success i e n codewords (containing d data bytes) are received with two or lesser errors and bit error rate, for different d is shown in Figure 3 10 From the graph, it is obvious that the probability of success is more than 0 99 for bit error rate of $3 * 10^{-3}$ and approaches to 1 at $2 * 10^{-3}$ Hence, it can be assumed, for a channel which provides better bit error rate than $2 * 10^{-3}$, that the graph 3 9 shows the actual data rate available

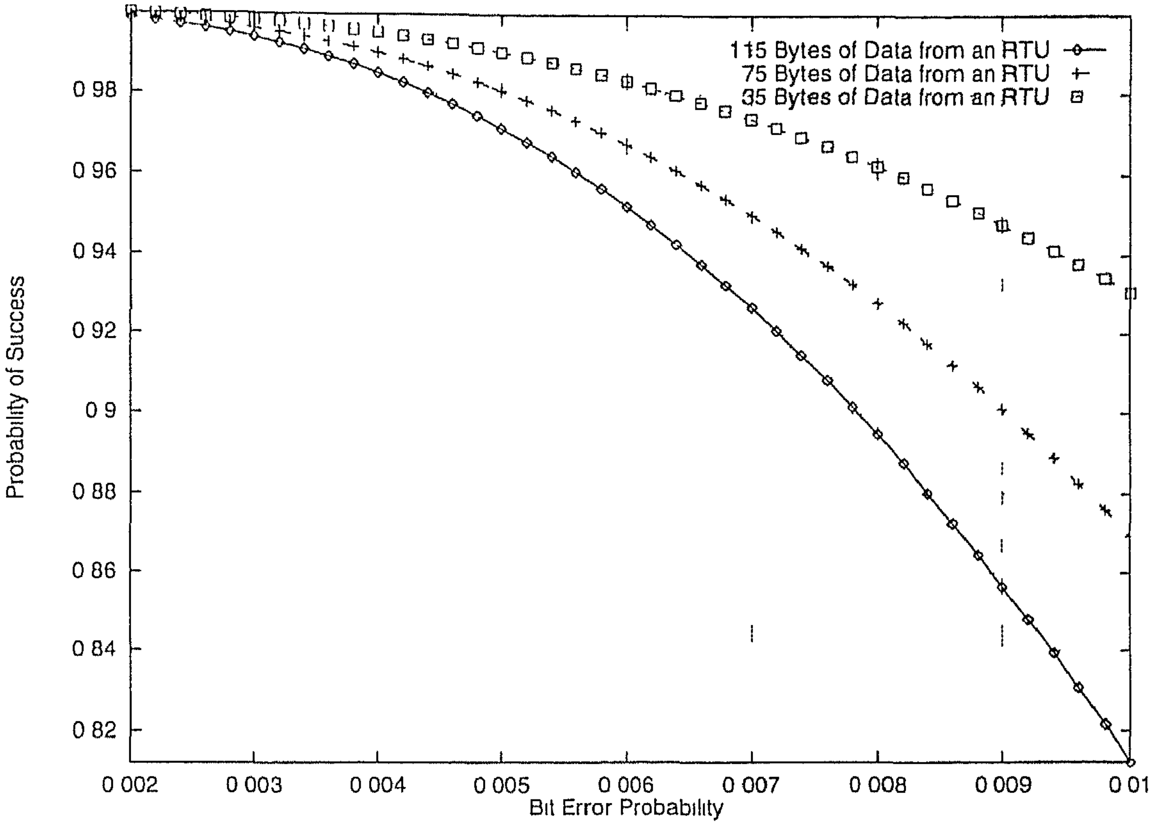


Figure 3 10 Probability of Success Vs Bit Error Rate

3 7 Discussion

In this chapter, we proposed a communication protocol for WNDMC As is obvious from the description the protocol has very low complexity and it provides sufficient data rate for low data rate applications The capacity is also found enough to meet the requirement of the power distribution system as the scheme can be used to poll about 50 RTUs (approximately 200 bytes from each RTU) every 5 minutes In ideal conditions each RTU can send approximately 215 bytes on each poll command from the master station If the data from each RTU is limited to maximum 115 bytes, the polling interval can be reduced to about 166 seconds

Chapter 4

Implementation Details

4.1 Introduction

The necessary infrastructure needed for point to multipoint communication between the master station and the RTUs is shown in Figure 2.1 and 2.2. The information to be transmitted from any network node passes through some operations as described in chapter 3 and then the data is transmitted over the wireless channel. The receiver receives the transmission and decodes the information from the data.

Since the hardware needed for wireless data transmission and reception is not available, we have implemented necessary hardware, and software on PC/XTs which does the necessary processing over the data to put it into the modified POCSAG format and transmits (receives) data over a synchronous wired channel.

The serial ports provided with the PCs are for asynchronous communication i.e. data is transmitted on character by character basis, each character with some start and stop bits. The transmission in the modified POCSAG format is also asynchronous. However, it requires that each block of data, which may contains several codewords each codeword of four bytes, should be transmitted synchronously. Keeping in view this requirement of the designed netwok, a serial interface card has been designed and implemented. The details of this interface card are discussed in the following section.

4 2 Hardware Implementation

4 2 1 Serial Synchronous Interface

To design the interface card we considered that it should be able to support full duplex synchronous communication as two independent channels are available for forward and reverse communication The maximum data rate supported by POCSAG is 2 4 Kbps Hence, flexibility should provided to choose different data rates in the required range At the same time, multiple addresses for the ICs in use should be provided to avoid any possible address conflict For high data rate applications, polling or flexibility to use diffrent interrupts for data reception and transmission should provided Since the card is to be implemented, all the ICs in the design should be available

For synchronous operation, popular and widely used IC 8251A, the *Programmable Communication Interface*, has been selected It can provide full duplex synchronous communication upto 64 Kbps To control transmission rate of 8251A, it is neccessary to control the clock rate provided to it This clock can be provided either by an external clock generator or PC clock can be divided by an appropriate circuitry In the circuit, IC 8253 5, the *Programmable Interval Timer*, is being used to divide the PC clock to generate clock for the 8251A

Since the 8253 5 can handle maximum 2 6 MHz frequency, it is necessary to divide PC clock before connecting it to 8253 5 IC 74LS93, *Binary Ripple Counter*, has been selected to divide PC clock To provide multiple addresses to 8251A and 8253 5, we have selected IC 74LS151 This is a 8 input mutiplexer For data transmission and reception, MC 3487 and MC 3486 are being used in the circuit [Tex87] These ICs support EIA defined RS 422 standard

4 2 2 Circuit description

Figure 4 1 shows the address decoder circuitry of the synchronous interface card The 8 input multiplexer is being used to provide four different addresses to 8253 5 and 8251A The address lines are input to the multiplexer and output of the multiplexer is controlled by DIP switches Hence, the state of DIP switches decides the address assigned to the

8253 5 and 8251A Address line A_{10} decides whether 8253 5 is addressed ($A_{10} = 1$) or 8251A ($A_{10} = 0$)

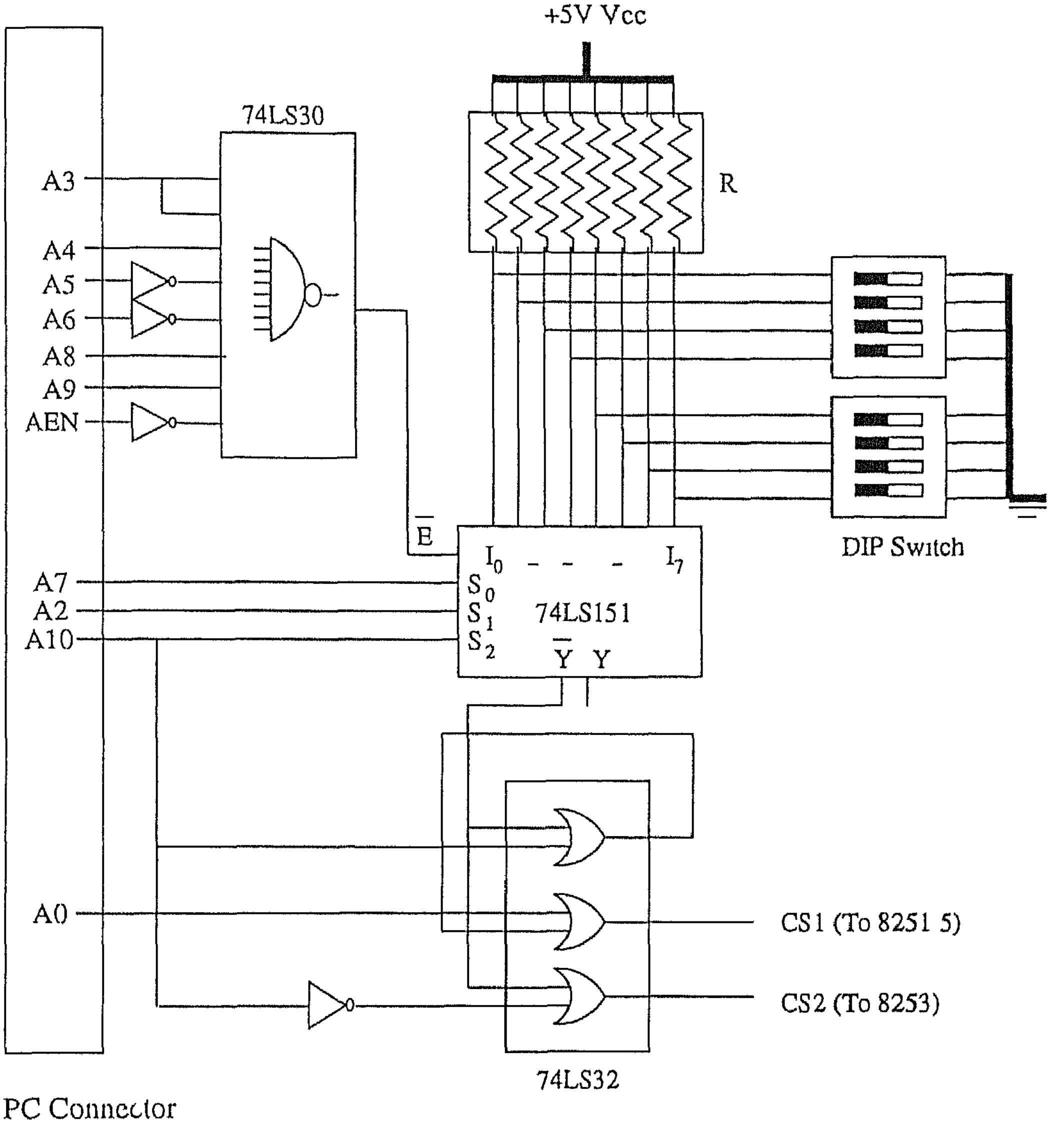


Figure 4 1 Address Decoder Circuit

Figure 4 2 shows the circuit diagram of communication interface The chip select signals (CS1 and CS2) are generated in the circuit shown in Figure 4 1 The data bus and I/O read and write signals of the PC are connected to 8253 5 and 8251A As shown in the figure, the PC clock is provided to binary ripple counter This counter can be used to divide input clock by a factor of 2, 4, 8 or 16 In the circuitry, it is being used in divide by 4 mode The output of the counter is connected to 8253 5 clock input

The two clock outputs of timer (OUT1 and OUT2) generate clocks for 8251A The OUT2 controls the transmission rate of 8251A and OUT1 provides clock to 8251A for its internal operations The clock rate of these clocks can be controlled by software This provides the user with the capability to select any desired rate for transmission

The TxRDY and RxRDY outputs of 8251A are being used to interrupt the system for data reception and transmission These outputs are fed to AND gates and tri state buffers to generate interrupt 3 or interrupt 4 Any combination of these interrupts can be used for data reception and transmission A DIP switch is provided to select an IRQ for data transmission and reception

Finally, the RS 422 standard is being used for data transfer Hence, serial input/output data pins and receiver/transmitter clocks of 8251A are connected to receiver (MC 3486) and driver (MC 3487) ICs A 9 pin connector is provided to interface this card with any other device which supports the RS 422 standard

4 2 3 Functioning

The functioning of the circuit is described as follows Initially, all the DIP switches are set in the desired state These switches decide the addresses of 8251A and 8253 5, and the interrupts used for transmission and reception Then, the complete functions of the card are programmed by the system's software The two ICs, 8251A and 8253-5, must be initialized by the software in order to use the card as a transmitter/receiver The 8253 5 is initialized prior to 8251A because it generates clock for 8251A

Since we are interested in synchronous mode, we restrict the following description to synchronous mode only The 8251A sends/receives data to/from the CPU on character by character basis It can be used to transmit/receive data on interrupt basis on on poll

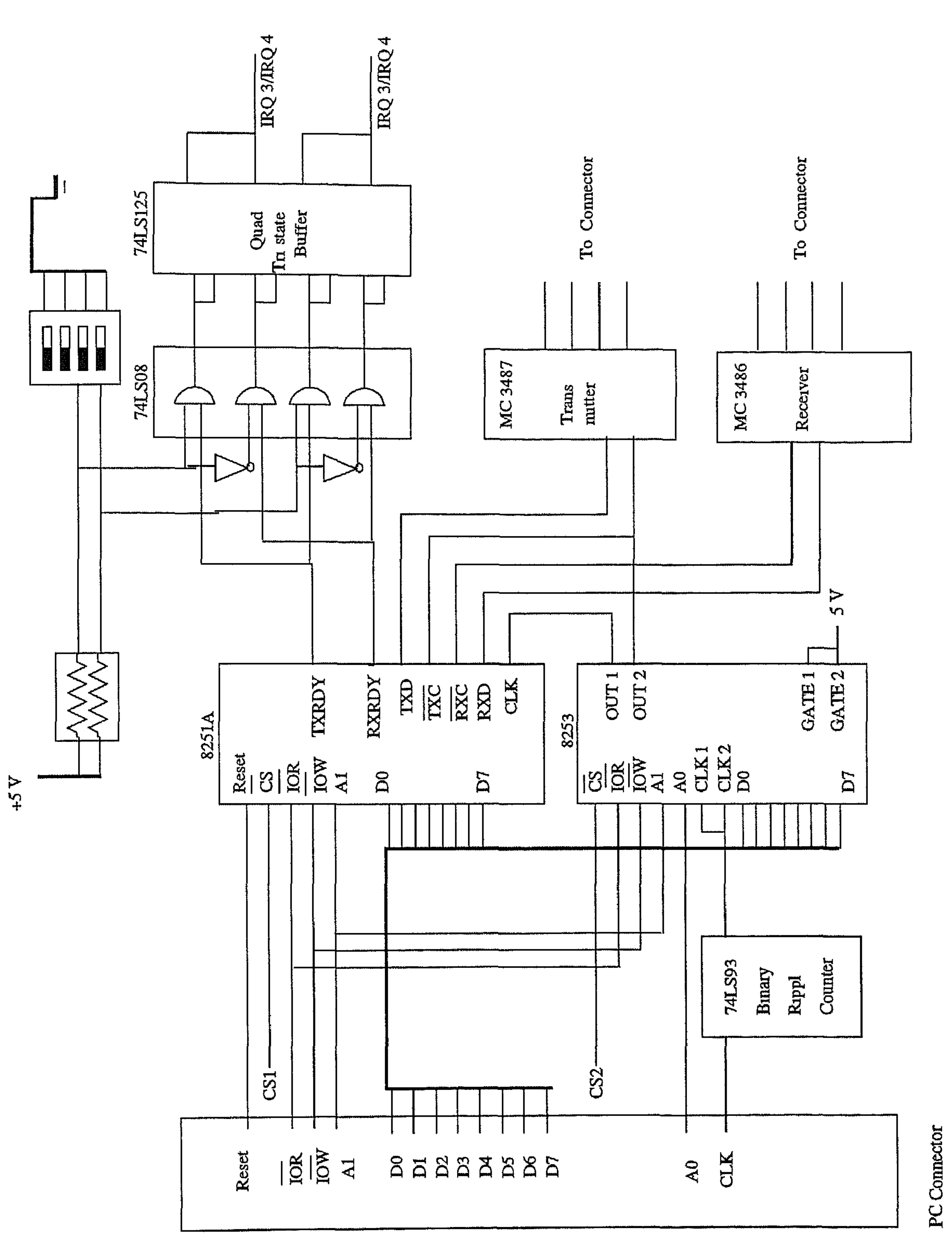


Figure 4 2 Communication Interface

basis. In the poll mode the CPU must check from time to time the status of status register of the 8251A. In receive mode the status register provides one bit to indicate whether there is data in the receiver buffer. Upon detecting data in receiver buffer, the CPU must run a read cycle to read the data from the buffer. If not read by the CPU the data will be lost upon reception of another character.

Similarly, the 8251A provides one bit to indicate that the transmitter is ready to accept a character from the CPU. The transmission starts with the first character received at the data port of the 8251A from the CPU. First one or two transmitted characters are always *sync characters*. Then it transmits the data character. After sending the first character to the 8251A, the CPU must continue to provide characters to 8251A at the desired rate otherwise the 8251A will insert some *sync characters* in the transmission.

In the interrupt mode the only difference is that the outputs of TxRDY and RxRDY pins are used to interrupt the CPU for transmission and reception. Whenever an interrupt comes i.e. RxRDY or TxRDY goes high, the CPU starts to serve a predefined *interrupt service routine*. This service routine, depending upon the interrupt number, sends or receives one character to/from the 8251A.

4.3 Software Implementation

The software is implemented on two PCs connected to each other with the synchronous interface described in the previous section. The setup is shown in Figure 4.3. One of the two PCs is assumed as the master and software on it provides the user or the operator with the capability to control the transmitter and receiver of this PC as well as of the other. This PC will be referred to as PCmain. The software on the other PC provides no control and once executed it is controlled by the PCmain. This PC will be referred to as PCslave. The complete software for the PCmain and PCslave is written in C language in TURBO C environment. The included files are **dos.h**, **conio.h** and **stdio.h**.
The main functions performed by the software are as follows:

- Initializes the 8251A and 8253-5.

- Encodes/decodes the information according to (31,21) BCH codes,

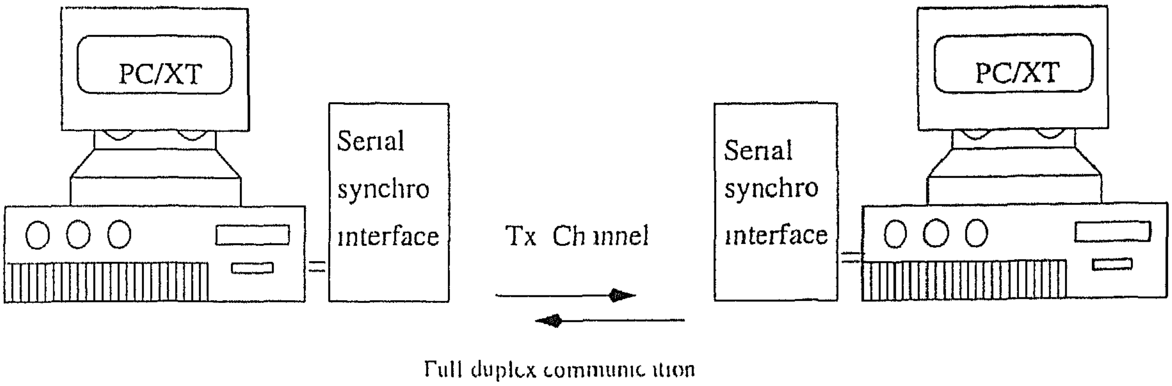


Figure 1.3 Testbed Architecture

- Transmits/receives data in the modified POCSAG format
- Provides control to operator

The software uses ISR (*Interrupt Service Routine*) and TSR (*Terminate but stay resident*) programs [Steve]. An ISR is a program which responds to an interrupt generated by a hardware device or a program. The ISR preserves the conditions of the computer when it interrupts the computer and returns the previous conditions when done. The ISR programming consists of installing the interrupt vector, which points to the *interrupt service routine*, into the interrupt vector table, handling the interrupt with *interrupt service routine*, and removing the interrupt vector.

A TSR is a program which reserves a block of memory for itself. Like an ISR, TSR program is also activated by software or hardware interrupt. The TSR program is executed as if it is a normal transient program and terminates by using a TSR function. When the program terminates it instructs DOS how much memory to reserve. The advantage of using ISR and TSR programs is that they allow the user to do other tasks on PC while they take neccessary action when an interrupt is generated.

4 3 1 PCmain

The software for PCmain is divided into two programs, a control program and a receiver program The control program provides the operator with complete control over the PCslave and the transmission channels It accepts commands from the operator and establishes sessions with the PCslave It also controls the baud rate of the transmission The receiver program receives data from the PCslave and displays it for the use of operator A detailed description of the functions of both programs is as follows

The control program consists of three modules, a *main*, an *encoder* and a *format* The *main* initializes the 8251A and 8253 5 accepts commands from the operator and transmits data over the channel The *encoder* takes address of PCslave and data to be transmitted from the *main* and encodes it according to (31 21) BCH codes The *format* takes encoded data from the *encoder* and puts the data in a buffer in the format defind in section 3 3 1 The *format* also takes care of the preamble and maintains the *frame structure*

The control program initializes the 8253 5 to generate clocks for 8251A which controls the data transmission rate from the PCmain The operator can control the data transmission rate by changing the clock rate of 8253 5 Then it initializes the 8251A for synchronous mode, 8 bit character, no parity and two *sync characters* This provides synchronous transmission of data without a single bit insertion in the data The 8251A doesn't start transmission until it gets a *command instruction word* at command port to set the transmitter on and a character at the data port Now the system is ready to accept operator's command

The program requires the information of the type of session to be established, address(s) of receiver(s) and command words (if necessary) from the operator The types of session, which can be established by the operator, have been described in section 3 3 1 For polling and acknowledgement sessions, it needs only the addresses of the receivers For other two sessions it asks for the data (command words in ascii characters) to be sent Before transmitting the data it does the following operations

The program takes the address of the receiver, encodes it according to (31,21) BCH codes, makes a 32 bit *address word* according to the format described in section 3 2 2 and puts it into a transmit buffer Then it takes data (max 20 bits at a time and pads 0 s if necessary) encode the data according to (31 21) BCH codes, makes a 32 bit message word and pushes it into the transmit buffer It also pushes a *timeword*, before message words in the buffer if required

Once all the data has been arranged in the buffer, it captures intterrupt 3 for data transmission and sends a *command instruction word* to 8251A to set its transmitter on On each interrupt generated by 8251A an *interrupt service routine* (ISR) is activated The procedure picks a character from the transmit buffer and sends it at the data port of 8251A After sending all the data from transmit buffer, the program stops the transmission and releases the interrupt 3

The receiver program is a TSR It consists of two modules, a *main* and a *decode* The *main* checks the status of 8251A If it finds the 8251A in reset mode, it initializes the 8251A for receive mode, otherwise it sends only the *command instruction word* to 8251A to set its receiver on It also captures the interrupt 4 of PC to receive data from the PCslave

Whenever the PCslave sends data interrupt 4 is generated This activates an *interrupt service routine* (ISR) which reads a character from the data port of 8251A and puts this character into a receiver buffer On detecting end of transmission, the ISR activates the TSR The ISR which is actually the *decode* picks four characters from the buffer to perform reverse operation of the *transmitter* and *encoder* It recognizes the address of the PCslave and decodes the data to display it for the operator

4 3 2 PCslave

The PCslave software is a TSR and once executed the operator has no control over it The program consists of four modules, a *main*, a *sdecoder*, a *sformat* and a *sencoder*

When the program is executed it initializes the 8253 5 and 8251A, captures interrupt 3 for receiving data from the PCmain and after that it terminates The 8251A receives data from the PCmain and generates interrupt 3 An *interrupt service routine* reads data from the data port of 8251A and puts it in a receiver buffer After receiving all the data, decoding is done The program starts search for the defined address and if any address is detected in the data, it takes action accordingly. This has already been described in the Chapter 3. The program also displays the data (command words) received with Ind_Add and Grp_Add. In response to poll, it sends the contents of a "data" file. The *sencoder* and the *sformat* put the data in a transmit buffer in the *message word* format. Then the *sencoder* captures interrupt 4 for data transmission and sends a *command instruction word* to the 8251A to set its transmitter on. Now, the data is transmitted by an interrupt subroutine. After sending all the data transmission is stoped and the interrupt 4 is released.

4.4 Discussion

In this chapter we presented the details of hardware and software implementation. The setup was tested for difficent inputs and it was found satisfactory for bit rate of more than 4.2Kbps.

The hardware was first tested using the debug utility of DOS and then it was used in the setup. It was found functioning satisfactorily upto the desired data rate of 4.2 Kbps. The software was first tested on UNIX machine for BCH decoding and encoding functions. Than different modules of the programs were tested. After that we used this software to provide two way synchronous communication between the two PCs. As discussed in the chapter, it provided some of those facilities on the PC which are expected to be a part of the master station. We also expect that the setup can be used for wireless communication between the two PCs provided the appropriate modems and receiver/transmitter units.

Chapter 5

Conclusion and Suggestions for Future Work

5.1 Conclusion

In the thesis, we proposed a low cost, low data rate wireless network and a communication scheme for distributed data acquisition and, monitoring and control of geographically dispersed objects. We also implemented necessary hardware and software for modified POCSAG communication scheme.

First, we assumed the design specifications of the network from available communication capacity and typical scenario of power distribution automation. We looked upon various wireless techniques which may suit the requirements of WNDMC. Considering the architecture and data rate requirements of the system, available frequency band, cost of network and some other factors, we proposed a network based on forward radiopaging (POCSAG) and return walkie talkie radio data link. Since, the POCSAG standard provides for one way communication, we modified it to meet the requirements of a two way communication network. We suggested that in the network, the master station and the RTUs should have a master slave relationship. We modified the roll call polling for better channel utilization and suggested a group call scheme to collect system information at the master station. The radiopaging itself provides error detection and error correction capability to the receiver. However, only error detection and correction is not sufficient for the control applications Over the existing radiopaging we suggested an error handling procedure which ensures reliable data delivery at the RTUs

Then we proposed a communication protocol based on these techniques The protocol exploits the capabilities of existing radiopaging communication and provides for full duplex reliable communication between the master station and the RTUs Under some reasonable assumptions we calculated the maximum capacity of the designed network and communication protocol

From the thesis we conclude that the suggested network can be implemented with low cost for monitoring and control of geographically dispersed equipments The graph, shown in Figure 3 10 showes the relationship between the total number of bytes that can be collected from each RTUs and polling interval for 10, 30 and 50 RTUs under the given assumptions It is obvious from the graph that the network provides sufficient data rate on reverse channel to poll 115 bytes from 50 RTUs at a polling interval of 166 seconds Since in power distribution system the expected data rate requirements from each unmanned transformer (RTU) to master station is approximately 100 bytes per 5 minutes and the number of RTUs under a 33/11 KV substation are approximately 50 [KiRe] we expect that the network can successfully be implemented to meet the requirement of power distribution system

5 2 Future Work

The area of a distributed monitoring and control network is very vast We addressed only a small area viz a low cost wireless network for monitoring and control of distributed objects Inspite of our efforts, we feel that further work is required in the following directions

The scheme was implemented over a wired channel for the PCs We suggest that the same approach can be followed to implement it over a wireless network Actually, the same setup can be used for this purpose with appropriate transmitter/receiver units and modems

The software and hardware provided synchronous communication over the channel

However, software is also needed for control applications. Depending upon the requirements of an application, software can be developed. The development of master station software requires system behavior knowledge and knowledge of the communication protocol and its flexibilty and capability.

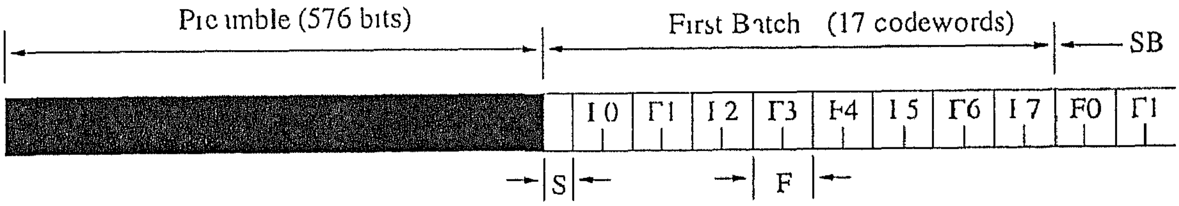
We disscussed only a few things about the RTUs, but the development of an appropriate RTU for a particular application require a lot of hardware and software knowledge. To get the maximum benefit of the described scheme, appropriate RTUs must be developed.

Appendix A

A 1 Radiopaging Code Standard

A 1 1 Code and format

A transmission consists of preamble followed by batches of complete codewords, each batch beginning with a synchronization codeword (SC) Transmission ceases when there are no further calls The format of transmission is shown in the figure A 1



S sync word
F one frame (2 codewords)
SB second batch

Figure A 1 Signals Format

Each transmission starts with a preamble to aid the receivers to attain bit synchronization The preamble is a pattern of reversals 101010 repeated for a period of atleast 576 bits i e the duration of a batch plus a code word

The preamble gives the receivers designed opportunity to save battery power The receiver can be turned on for a few milliseconds and then turned off for about 1 second if no preamble is detected When detected, preamble provides fast bit synchronization

A.1.2 Batch Structure

Codewords are structured into batches which comprise a synchronization codeword followed by 8 frames each containing 2 codewords. The frames are numbered from 0 to 7 and receivers population is devided into 8 groups. Thus each receivers is allocated to one of the 8 frames according to 3 least significant bits of its 21 bit identity i.e. 000 = frame 0 ....,111 = frame 7 and only examines address codeword in that frame. Therefore each receivers address must be transmitted only in the allocated frame.

This frame structure within a batch not only multiplies the address possibilities of each codeword by 8 but also offers yet another means of battery saving within the receivers, since the receiver need only be turned on during the SC and its particular frame.

Message codewords for any receiver may be transmitted in any frame but follow, directly the associated codeword. A message may consist of any number of codewords transmitted consecutively and may embrace more than one batches but the SC must not be displaced by message codewoeds i.e. normal batch structure is always maintained. Message termination is indicated by next address codeword or idle codeword. There is atleast one address or idle codeword between the end of one message and the address codeword belonging to the next message.

A.1.3 Types of Codeword

Codewords contains 32 bits which are transmitted with the most significant bit first. General structure of a codeword is illustrated in fig. Different types of codewords are given below.

1. Synchronization Codeword

This codeword has very low correlation with the preamble. Its first 31 bits are pseudo random sequence which can be generated from a 5 stage feedback shift register. This is a valid codeword with the structure given below.

01111100110100100001010111011000

2 Address codewords

The address codeword always has its first bit (flag bit) zero This distinguishes it from message codeword Bits 2 19 are address bits corresponding to 18 most significant bits of a 21 bit identity assigned to the receivers Bits 20 21 are two function bits which are used to select the required address from the four assigned to the receivers Bit 22 31 are parity check bits and the final bit is chosen to give even parity

3 Message Codewords

A message codeword always starts with a 1 (the flag bit) and the whole message always follows directly after the address codeword The framing rules of the code format do not apply to the message and message codeword continue until terminated by the transmission of a new address word or an idle codeword Each message displaces atleast one address codeword or an idle codeword and the displaced address codewords are delayed and transmitted in the next available appropriate frame

Message codewords have 20 message bits viz bit 2 21 inclusive and these are followed by the parity check bits

4 Idle Codeword

In the absence of an address codeword or message codeword an idle code word is transmitted The idle codeword is a valid codeword, which must not be allocated to any receivers and has the following structure

01111010100010011100000110010111

A 1 4 Codeword Generation

Each codeword has 21 information bits, which correspond to the coefficients of a polynomial having terms from x^{30} down to x^{10} Generator polynomial used to generate the codewords is $g(x) = x^{10} + x^{9} + x^{8} + x^{6} + x^{5} + x^{3} + 1$ The message polynomial is devided by the generator polynomial to give check bits corresponding to the coefficient of the terms from x^9 to x^0. The complete block consisting of the information bits followed by the check bits correspond to the coefficient of a polynomial which is integrally devisible in modulo 2 fashion by the generator polynomial.

To 31 bits of the block is added one additional bit to provide an even bit parity check of the whole codeword. Thus the Hamming distance of the code is 6. This makes enable to detect any five bit errors or any one error burst of length not exceeding 11 bits or to correct any 2 errors or any error burst not exceeding 4 bits.

A.2 PCB layout

The placement of ICs on the PCB is shown in Figure A.2.

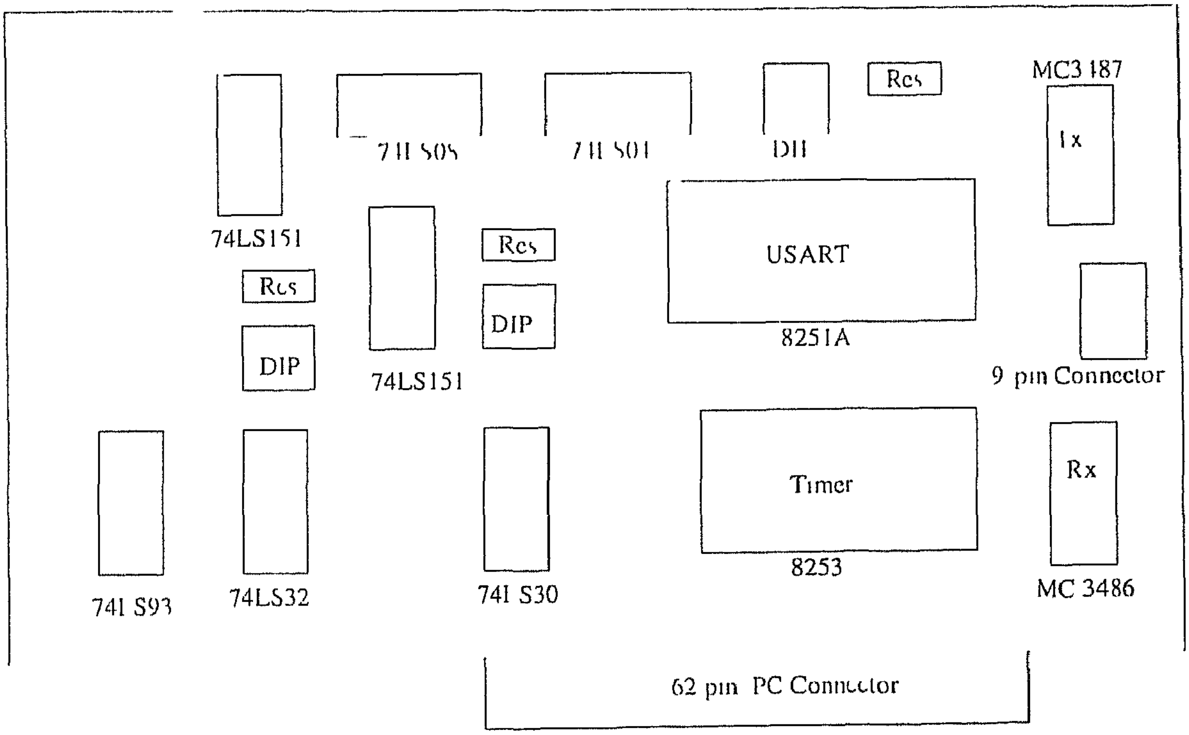


Figure A.2: PCB layout

As discussed in chapter 4, the ICs 8251A and 8253-5 have four addresses. Any of the address can be selected with the DIP switches provided. If more than one switches are on the IC will be activated at more than one addresses. So, care must be taken to switch on only one switch

The addresses available for the 8251A and 8253-5 are shown in the following table

Addresses for 8253-5

Command Port	Counter 2	counter 1	counter 0
71BH	71AH	719H	718H
71FH	71EH	71DH	71CH
79BH	79AH	799H	798H
79FH	79EH	79DH	79CH

Addresses for 8251A

Data Port	Command Port
318H	31AH
31CH	31EH
398H	39AH
39CH	39EH

Bibliography

[AnR96] Rajanandam A and Subramaniam B Remote Alarm Monitoring System for Unmanned Substations *Distribution Automation/DSM 96 Conference Papers pp 5 91 5 107*

[KrRe] Srivathsan, K R and Reddy, P V K "Communication & Networking Aspects of Distribution Automation *Internal Paper DA/TDM EE Deptt, IIT Kanpur*

[Dav94] Bantz, David F and Bauchot F J 'Wireless LAN Design Alternatives", *IEEE Networks, March/April 94 pp 26 33*

[Vic87] Victor O K Li Multiple Access Communication Networks *IEEE, Communication Magazine June 87, Vol 25 No 6 pp 34 41*

[KrJ96] Prasad, Krishna V and Advani J S , " Distribution and Automation in Indian Power Utilities The Real Scenario *Distribution Automation/DSM '96 Conference Papers pp 5 1 5 10*

[Schw] Schwartz M 'Telecommunication Networks Protocols, Modeling and Analysis" *Addison Wesley Publishing Company California 1988*

[Steve] Al Steves , 'Turbo C Memory Resident Utilities, Screen I/O and Programming Techniques' , *Tech Publications Singapore, 1989*

[Meye] Meyers, Robert A , Editor "Encyclopedia of Telecommunications", *Academic Press, Inc , California, 1989, pp 109 111*

[Blah] Blahut Rechard E 'Theory and Practice of Error Control Codes", *Prentice Hall, New Jersey, 1986*

[GalB] Gallager, R and Bertsekas D Data Networks", *Prentice Hall of India Delhi, 1994*

[CCIR] CCIR Paging Code No 1 POCSAG , *The Book of the CCIR Radiopaging Code No 1 , Available from*
Radio Design Group Inc 3810 Almar Road Grants Pass, OR 97527

[InC93] Connectivity *Intel pp 2 1 2 25 1993*

[InP93] Peripheral Components', *Intel pp 3 51 3 61 ,1993*

[PCref] IBM PC/AT Reference Mannual *Technical Reference*

[Sig86] 'TTL Products Data Mannual *Signetics 1986*

[Tex87] Interface Circuit Data Book *Texas Instruments ' pp 1987*

[GSM] 'The GSM Tutorial',
URL http //www webproforum com/ericsson/index html

[John] John Scourias, University of Waterloo, "Overview of the GSM Cellular System",
URL http //ccnga uwaterloo ca/ jscouria/GSM/trio html

[Qual] OmniTRACS Product and Technology'
URL http //www qualcomm com/OmniTRACS/products/system html

[Sca91] Excerpt from Energy & Environmental News", January 1991,
URL http //energy nfesc navy mil/energy/neesa/scada1 html

[Spre] 'The principles of Spread Spectrum communication2
URL http //olt et tudelft nl/ glas/ssc/techn/techniques html

[Trunk] "The Growth of Low Cost Radio Trunking Systems in Latin America",
URL http //www smartrunk com/manual/chapter1 html

[AMPS] The Radio Telephony Tutorial
URL http //www iec org/tutor/nortel/index htm